

Diophantine Triples and k -Generalized Fibonacci Sequences

Clemens Fuchs¹  · Christoph Hutle¹ ·
Florian Luca^{2,3} · László Szalay^{4,5}

Received: 26 February 2016 / Revised: 17 June 2016 / Published online: 4 August 2016
© The Author(s) 2016. This article is published with open access at Springerlink.com

Abstract We show that if $k \geq 2$ is an integer and $(F_n^{(k)})_{n \geq 0}$ is the sequence of k -generalized Fibonacci numbers, then there are only finitely many triples of positive integers $1 < a < b < c$ such that $ab + 1$, $ac + 1$, $bc + 1$ are all members of $\{F_n^{(k)} : n \geq 1\}$. This generalizes a previous result where the statement for $k = 3$ was proved. The result is ineffective since it is based on Schmidt's subspace theorem.

Keywords Diophantine triples · Generalized Fibonacci numbers · Diophantine equations · Application of the Subspace theorem

Mathematics Subject Classification 11D72 · 11B39 · 11J87

Communicated by Emrah Kilic.

✉ Clemens Fuchs
clemens.fuchs@sbg.ac.at

Christoph Hutle
christoph.hutle@gmx.at

Florian Luca
florian.luca@wits.ac.za

László Szalay
szalay.laszlo@nyme.hu

¹ University of Salzburg, Hellbrunner Str. 34/I, 5020 Salzburg, Austria

² University of Witwatersrand, Johannesburg, South Africa

³ Centro de Ciencias Matemáticas UNAM, Morelia, Mexico

⁴ J. Selye University, Hradna ul. 21, 94501 Komarno, Slovakia

⁵ University of West Hungary, Sopron, Hungary

1 Introduction

There are many papers in the literature concerning Diophantine m -tuples which are sets of m distinct positive integers $\{a_1, \dots, a_m\}$ such that $a_i a_j + 1$ is a square for all $1 \leq i < j \leq m$ (see [4], for example). A variation of this classical problem is obtained if one changes the set of squares by some different subsets of positive integers like k -powers for some fixed $k \geq 3$, or perfect powers, or primes, or members of some linearly recurrent sequence, etc. (see [7, 12–14, 18]). In this paper, we study this problem with the set of values of k -generalized Fibonacci numbers for some integer $k \geq 2$. Recall that these numbers denoted by $F_n^{(k)}$ satisfy the recurrence

$$F_{n+k}^{(k)} = F_{n+k-1}^{(k)} + \dots + F_n^{(k)}$$

and start with $0, 0, \dots, 0$ ($k-1$ times) followed by 1. Notationwise, we assume that $F_i^{(k)} = 0$ for $i = -(k-2), -(k-1), \dots, 0$, and $F_1^{(k)} = 1$. For $k = 2$ we obtain the Fibonacci numbers and for $k = 3$ the sequence of Tribonacci numbers. The result is the following:

Theorem 1 *Let $k \geq 2$ be fixed. Then there are only finitely many triples of positive integers $1 < a < b < c$ such that*

$$ab + 1 = F_x^{(k)}, \quad ac + 1 = F_y^{(k)}, \quad bc + 1 = F_z^{(k)} \quad (1)$$

hold for some integers x, y, z .

Our result generalizes the results obtained in [8], [11] and [13], where this problem was treated for the cases $k = 2$ and $k = 3$. In [13] it was shown that there does not exist a triple of positive integers a, b, c such that $ab + 1, ac + 1, bc + 1$ are Fibonacci numbers. In [11] it was shown that there is no Tribonacci Diophantine quadruple, that is a set of four positive integers $\{a_1, a_2, a_3, a_4\}$ such that $a_i a_j + 1$ is a member of the Tribonacci sequence (3-generalized Fibonacci sequence) for $1 \leq i < j \leq 4$, and in [8] it was proved that there are only finitely many Tribonacci Diophantine triples. In the current paper, we prove the same result for all such triples having values in the sequence of k -generalized Fibonacci numbers.

For the Proof of Theorem 1, we proceed as follows. In Sect. 2, we recall some properties of the k -generalized Fibonacci sequence $F_n^{(k)}$ which we will need and we prove two lemmata. The first lemma shows that any $k-1$ roots of the characteristic polynomial are multiplicatively independent. In the second lemma, the greatest common divisor of $F_x^{(k)} - 1$ and $F_y^{(k)} - 1$ for $2 < y < x$ is estimated. In Sect. 3, we assume that the Theorem 1 is false and give, using the Subspace theorem, a finite expansion of infinitely many solutions. In Sect. 4, we use a parametrization lemma which is proved by using results about finiteness of the number of non-degenerate solutions to S -unit equations. Applying it to the finite expansion, this leads us to a condition on the leading coefficient, which turns out to be wrong. This contradiction is obtained by showing that a certain Diophantine equation has no solutions; this last Diophantine equation has been treated in particular cases in [2] and [16].

2 Preliminaries

There are already many results in the literature about $(F_n^{(k)})_{n \geq 0}$. We will only use what we need, which are the following properties. The sequence $(F_n^{(k)})_{n \geq 0}$ is linearly recurrent of characteristic polynomial

$$\Psi_k(X) = X^k - X^{k-1} - \dots - X - 1.$$

The polynomial $\Psi_k(X)$ is separable and irreducible in $\mathbb{Q}[X]$ and the Galois group thus acts transitively on the roots, which we denote by $\alpha_1, \dots, \alpha_k$. If k is even or prime, the Galois group is certainly S_k (see [16] for these statements). The polynomial $\Psi_k(X)$ has only one root, without loss of generality assume that this root is $\alpha_1 > 1$, which is outside the unit disk (formally, this root depends also on k , but in what follows we shall omit the dependence on k on this and the other roots of $\Psi_k(X)$ in order to avoid notational clutter). Thus,

$$\Psi_k(X) = \prod_{i=1}^k (X - \alpha_i), \quad \text{where } |\alpha_i| < 1, \quad i = 2, \dots, k.$$

Observe that $\alpha_1 \alpha_2 \dots \alpha_k = (-1)^{k-1}$. Note also that

$$\Psi_k(X) = X^k - (X^{k-1} + \dots + 1) = X^k - \frac{X^k - 1}{X - 1} = \frac{X^{k+1} - 2X^k + 1}{X - 1},$$

a representation which is sometimes useful. Furthermore,

$$2 - \frac{1}{k} < \alpha_1 < 2 \tag{2}$$

(see Lemma 3 in [3]). The Binet formula of $(F_n^{(k)})_{n \geq 0}$ is given by

$$F_n^{(k)} = \sum_{i=1}^k f_i \alpha_i^n \quad \text{for all } n \geq 0, \tag{3}$$

where

$$f_i = \frac{(\alpha_i - 1)\alpha_i^{-1}}{2 + (k+1)(\alpha_i - 2)}, \quad i = 1, \dots, k \tag{4}$$

(see Theorem 1 in [3]). We have

$$|F_n^{(k)} - f_1 \alpha_1^n| < \frac{1}{2} \quad \text{for all } n \geq 1 \tag{5}$$

and

$$f_1 < 1 \tag{6}$$

(see Theorem 2 in [3]). We also need the fact that

$$\alpha_1^{n-2} < F_n^{(k)} < \alpha_1^{n-1} \quad (7)$$

(see [1]).

Furthermore, the following property is of importance; it follows from the fact that there is no non-trivial multiplicative relation between the conjugates of a Pisot number (cf. [15]). Since in our case it is rather easy to verify, we shall present a proof of what we need.

Lemma 1 *Each set of $k - 1$ different roots (e.g., $\{\alpha_1, \dots, \alpha_{k-1}\}$) is multiplicatively independent.*

Proof We shall prove the statement only for the set $\{\alpha_1, \dots, \alpha_{k-1}\}$. The general statement follows easily by the transitivity of the Galois Group of the irreducible polynomial $\Psi_k(X)$.

Let us denote by $\mathbb{L} := \mathbb{Q}(\alpha_1, \dots, \alpha_k)$ the splitting field of Ψ_k over \mathbb{Q} and by $\mathcal{O}_{\mathbb{L}}$ the ring of integers in \mathbb{L} . Note that the roots $\alpha_1, \dots, \alpha_k$ are certainly in the group of units $\mathcal{O}_{\mathbb{L}}^\times$ which follows from

$$\alpha_i^{-1} = (-1)^{k-1} (\alpha_1 \cdots \alpha_{i-1} \cdot \alpha_{i+1} \cdots \alpha_k)$$

for $i = 1, \dots, k$. The extension \mathbb{L}/\mathbb{Q} is Galois. We denote by d its degree and by $G := \text{Gal}(\mathbb{L}/\mathbb{Q})$ the Galois group of \mathbb{L} over \mathbb{Q} . Let $G = \{\sigma_1, \dots, \sigma_d\}$. We consider the map $\lambda : \mathcal{O}_{\mathbb{L}}^\times \rightarrow \mathbb{R}^d$ defined by $x \mapsto (\log |\sigma_1(x)|, \log |\sigma_2(x)|, \dots, \log |\sigma_d(x)|)$. Observe that by the product formula we have for $x \in \mathbb{L}^\times$ that

$$\prod_{v \in M_{\mathbb{L}}} |x|_v = 1;$$

and for $x \in \mathcal{O}_{\mathbb{L}}^\times$ this leads to

$$\prod_{\substack{v \in \mathbb{L} \\ v \nmid \infty}} |x|_v = 1$$

since for every finite place v we have $|x|_v = 1$. This means that the image of λ lies in the hyperplane defined by $X_1 + \dots + X_d = 0$ of \mathbb{R}^d .

We will use the property that λ is a homomorphism (see e.g., [17]). So if we can prove that the $k - 1$ vectors $\lambda(\alpha_1), \dots, \lambda(\alpha_{k-1})$ are linearly independent, this will prove the statement.

Since Ψ_k is irreducible over \mathbb{Q} , the Galois group G of \mathbb{L} over \mathbb{Q} acts transitively on $\{\alpha_1, \dots, \alpha_k\}$, i.e., for each $i = 1, \dots, k$ there is some Galois automorphism which sends α_i to α_1 ; without loss of generality let $\sigma_1, \dots, \sigma_k$ be such that $\sigma_i(\alpha_i) = \alpha_1$. Observe that $\sigma_i^{-1}(\alpha_1) = \{\alpha_i\}$ for $i = 1, \dots, k$. We have

$$\lambda(\alpha_1) = (\log |\alpha_1|, \log |\sigma_2(\alpha_1)|, \dots, \log |\sigma_{k-1}(\alpha_1)|, \dots),$$

$$\begin{aligned}\lambda(\alpha_2) &= (\log |\sigma_1(\alpha_2)|, \log |\alpha_1|, \dots, \log |\sigma_{k-1}(\alpha_2)|, \dots), \\ &\vdots \\ \lambda(\alpha_{k-1}) &= (\log |\sigma_1(\alpha_{k-1})|, \log |\sigma_2(\alpha_{k-1})|, \dots, \log |\alpha_1|, \dots).\end{aligned}$$

We will show that the matrix $(\log |\sigma_i(\alpha_j)|)_{i=1, \dots, k-1; j=1, \dots, k-1}$ consisting of the first $k-1$ entries of these $k-1$ vectors has rank $k-1$ implying the statement of the lemma.

Observe now that $\alpha_1 \cdots \alpha_k = (-1)^{k-1}$ and thus $|\sigma_i(\alpha_1 \cdots \alpha_k)| = 1$ for all $i = 1, \dots, k-1$. It follows that $\sum_{j=1}^k \log |\sigma_i(\alpha_j)| = 0$ and thus

$$\sum_{j=1}^{k-1} \log |\sigma_i(\alpha_j)| = -\log |\sigma_i(\alpha_k)| > 0$$

for $j = 1, \dots, k-1$ and all $i = 1, \dots, k-1$. Hence the transpose of the matrix above is strictly diagonal-dominant since the diagonal entries, which are all equal to $\log |\alpha_1|$, are positive, all other entries are negative, and each row-sum (in the transpose matrix) of all off-diagonal entries is in absolute value less than the corresponding diagonal entry. It follows that the matrix is regular, which is what we wanted to show. \square

Finally, we prove the following result, which generalizes Proposition 1 in [8]. Observe that the upper bound depends now on k .

Lemma 2 *Let $x > y \geq 3$. Then*

$$\gcd(F_x^{(k)} - 1, F_y^{(k)} - 1) < \alpha_1^{\frac{kx}{k+1}}. \quad (8)$$

Proof We may assume that $y \geq 4$, since for $y = 3$, we get $F_y^{(k)} - 1 = 1$, and there is nothing to prove. We put $d = \gcd(F_x^{(k)} - 1, F_y^{(k)} - 1)$. Let κ be a constant to be determined later. If $y \leq \kappa x + 1$, then

$$d \leq F_y^{(k)} - 1 < F_y^{(k)} < \alpha_1^{y-1} \leq \alpha_1^{\kappa x}. \quad (9)$$

From now on, we assume that $y > \kappa x + 1$. Using (3) and (5), we write

$$\begin{aligned}F_x^{(k)} &= f_1 \alpha_1^x + \zeta_x, & |\zeta_x| &< 1/2, \\ F_y^{(k)} &= f_1 \alpha_1^y + \zeta_y, & |\zeta_y| &< 1/2.\end{aligned} \quad (10)$$

We put $\mathbb{K} = \mathbb{Q}(\alpha_1)$. We let $\lambda = x - y < (1 - \kappa)x - 1$, and note that

$$d \mid (F_x^{(k)} - 1) - \alpha_1^\lambda (F_y^{(k)} - 1) \text{ in } \mathbb{K}.$$

We write

$$d\eta = (F_x^{(k)} - 1) - \alpha_1^\lambda (F_y^{(k)} - 1),$$

where η is some algebraic integer in \mathbb{K} . Note that the right-hand side above is not zero, for if it were, we would get $\alpha_1^\lambda = (F_x^{(k)} - 1)/(F_y^{(k)} - 1) \in \mathbb{Q}$, which is false for $\lambda > 0$. We compute norms from \mathbb{K} to \mathbb{Q} . Observe that

$$\begin{aligned} \left| (F_x^{(k)} - 1) - \alpha_1^\lambda (F_y^{(k)} - 1) \right| &= |(f_1 \alpha_1^x + \zeta_x - 1) - \alpha_1^\lambda (f_1 \alpha_1^y + \zeta_y - 1)| \\ &= |\alpha_1^\lambda (1 - \zeta_y) - (1 - \zeta_x)| \\ &\leq \frac{3}{2} \alpha_1^\lambda - \frac{1}{2} < \frac{3}{2} \alpha_1^\lambda < \alpha_1^{\lambda+1} \leq \alpha_1^{(1-\kappa)x}. \end{aligned}$$

In the above, we used the fact that

$$-1/2 < \zeta_x, \zeta_y < 1/2$$

(see (5)) as well as (2). Further, let σ_i be any Galois automorphism that maps α_1 to α_i . Then for $i \geq 2$, we have

$$\begin{aligned} \left| \sigma_i \left((F_x^{(k)} - 1) - \alpha_1^\lambda (F_y^{(k)} - 1) \right) \right| &= \left| (F_x^{(k)} - 1) - \alpha_i^\lambda (F_y^{(k)} - 1) \right| \\ &< F_x^{(k)} - 1 + F_y^{(k)} - 1 < \alpha^{x-1} + \alpha^{y-1} - 2 \\ &< \alpha^{x-1} (1 + \alpha^{-1}) \leq \alpha^x. \end{aligned}$$

We then have

$$\begin{aligned} d^k &\leq |N_{\mathbb{K}/\mathbb{Q}}(d\eta)| \\ &\leq \left| N_{\mathbb{K}/\mathbb{Q}} \left((F_x^{(k)} - 1) - \alpha_1^\lambda (F_y^{(k)} - 1) \right) \right| \\ &= \left| \prod_{i=1}^k \sigma_i \left((F_x^{(k)} - 1) - \alpha_1^\lambda (F_y^{(k)} - 1) \right) \right| \\ &< \alpha_1^{(1-\kappa)x} (\alpha_1^x)^{k-1} = \alpha_1^{(k-\kappa)x}. \end{aligned}$$

Hence,

$$d \leq \alpha_1^{(1-\kappa/k)x}. \quad (11)$$

In order to balance (9) and (11), we choose κ such that $\kappa = 1 - \kappa/k$, giving $\kappa = k/(k+1)$, and the lemma is proved. \square

3 Parametrizing the Solutions

In order to simplify the notations, we shall from now onwards write F_n instead of $F_n^{(k)}$; we still mean the n th k -generalized Fibonacci number. The arguments in this section follow the arguments from [8]. We will show that if there are infinitely many solutions to (1), then all of them can be parametrized by finitely many expressions as given in (18) for c below.

We assume that there are infinitely many solutions to (1). Then, for each integer solution (a, b, c) , we have

$$a = \sqrt{\frac{(F_x - 1)(F_y - 1)}{F_z - 1}}, b = \sqrt{\frac{(F_x - 1)(F_z - 1)}{F_y - 1}}, c = \sqrt{\frac{(F_y - 1)(F_z - 1)}{F_x - 1}}.$$

From

$$\alpha_1^{x+y-2} \geq F_x F_y > (F_x - 1)(F_y - 1) \geq F_z - 1 \geq \alpha_1^{z-2} - 1 > \alpha_1^{z-3}$$

we see that $x + y > z - 1$ and thus $y \geq z/2$. In order to get a similar correspondence for x and z , we denote $d_1 := \gcd(F_y - 1, F_z - 1)$ and $d_2 := \gcd(F_x - 1, F_z - 1)$, such that $F_z - 1 \mid d_1 d_2$. Then we use Lemma 2 to obtain

$$\alpha_1^{x-1} > F_x > F_x - 1 \geq d_2 \geq \frac{F_z - 1}{d_1} \geq \frac{\alpha_1^{z-2} - 1}{\alpha_1^{\frac{kz}{k+1}}} > \alpha_1^{z - \frac{kz}{k+1} - 3}$$

and hence

$$x > \left(1 - \frac{k}{k+1}\right)z - 2,$$

which we can write as $x > C_1 z$ for some small constant $C_1 < 1$ (depending only on k), when z is sufficiently large.

Next, we do a Taylor series expansion for c which was given by

$$c = \sqrt{\frac{(F_y - 1)(F_z - 1)}{F_x - 1}}. \quad (12)$$

Using the power sum representations of F_x, F_y, F_z , we get

$$\begin{aligned} c &= \sqrt{f_1} \alpha_1^{(-x+y+z)/2} \\ &\cdot \left(1 + (-1/f_1)\alpha_1^{-x} + (f_2/f_1)\alpha_2^x \alpha_1^{-x} + \cdots + (f_k/f_1)\alpha_k^x \alpha_1^{-x}\right)^{-1/2} \\ &\cdot \left(1 + (-1/f_1)\alpha_1^{-y} + (f_2/f_1)\alpha_2^y \alpha_1^{-y} + \cdots + (f_k/f_1)\alpha_k^y \alpha_1^{-y}\right)^{1/2} \\ &\cdot \left(1 + (-1/f_1)\alpha_1^{-z} + (f_2/f_1)\alpha_2^z \alpha_1^{-z} + \cdots + (f_k/f_1)\alpha_k^z \alpha_1^{-z}\right)^{1/2}. \end{aligned}$$

We then use the binomial expansion to obtain

$$\begin{aligned} &(1 + (-1/f_1)\alpha_1^{-x} + (f_2/f_1)\alpha_2^x \alpha_1^{-x} + \cdots + (f_k/f_1)\alpha_k^x \alpha_1^{-x})^{1/2} \\ &= \sum_{j=0}^T \binom{1/2}{j} \left((-1/f_1)\alpha_1^{-x} + (f_2/f_1)\alpha_2^x \alpha_1^{-x} + \cdots + (f_k/f_1)\alpha_k^x \alpha_1^{-x}\right)^j + \mathcal{O}\left(\alpha_1^{-(T+1)x}\right), \end{aligned}$$

where \mathcal{O} has the usual meaning, using estimates from [9] and where T is some index, which we will specify later. Since $x < z$ and $z < x/C_1$, the remainder term can also be written as $\mathcal{O}(\alpha_1^{-T\|x\|/C_1})$, where $\|x\| = \max\{x, y, z\} = z$. Doing the same for y and z likewise and multiplying those expressions gives

$$c = \sqrt{f_1} \alpha_1^{(-x+y+z)/2} \left(1 + \sum_{j=1}^{n-1} d_j M_j \right) + \mathcal{O}(\alpha_1^{-T\|x\|/C_1}), \quad (13)$$

where the integer n depends only on T and where J is a finite set, d_j are non-zero coefficients in $\mathbb{L} := \mathbb{Q}(\alpha_1, \dots, \alpha_k)$, and M_j is a monomial of the form

$$M_j = \prod_{i=1}^k \alpha_i^{L_{i,j}(\mathbf{x})},$$

in which $\mathbf{x} = (x, y, z)$, and $L_{i,j}(\mathbf{x})$ are linear forms in $\mathbf{x} \in \mathbb{R}^3$ with integer coefficients which are all non-negative if $i = 2, \dots, k$ and non-positive if $i = 1$. Note that each monomial M_j is “small” that is there exists a constant $\kappa > 0$ (which we can even choose independently of k), such that

$$|M_j| \leq e^{-\kappa x} \quad \text{for all } j \in J. \quad (14)$$

This follows directly from

$$\begin{aligned} |M_j| &= |\alpha_1|^{L_{1,j}(\mathbf{x})} \cdot |\alpha_2|^{L_{2,j}(\mathbf{x})} \cdots |\alpha_k|^{L_{k,j}(\mathbf{x})} \\ &\leq (2 - 1/k)^{L_{1,j}(\mathbf{x})} \cdot 1 \cdots 1 \\ &\leq (3/2)^{-x} \\ &\leq e^{-\kappa x} \quad \text{for all } j \in J. \end{aligned}$$

Our aim of this section is to apply a version of the Subspace theorem given in [5] to show that there is a finite expansion of c involving terms as in (13); the version we are going to use can also be found in Sect. 3 of [10]. For the set-up—in particular the notion of heights—we refer to the mentioned papers.

We work with the field $\mathbb{L} = \mathbb{Q}(\alpha_1, \dots, \alpha_k)$ and let S be the finite set of infinite places (which are normalized so that the Product Formula holds, cf. [5]). Observe that $\alpha_1, \dots, \alpha_k$ are S -units. According to whether $-x + y + z$ is even or odd, we set $\epsilon = 0$ or $\epsilon = 1$ respectively, such that

$$\alpha_1^{(-x+y+z-\epsilon)/2} \in \mathbb{L}.$$

By going to a still infinite subset of the solutions, we may assume that ϵ is always either 0 or 1.

Using the fixed integer n (depending on T) from above, we now define $n+1$ linearly independent linear forms in indeterminates (C, Y_0, \dots, Y_n) . For the standard infinite place ∞ on \mathbb{C} , we set

$$l_{0,\infty}(C, Y_0, \dots, Y_{n-1}) := C - \sqrt{f_1 \alpha_1^\epsilon} Y_0 - \sqrt{f_1 \alpha_1^\epsilon} \sum_{j=1}^{n-1} d_j Y_j, \quad (15)$$

where $\epsilon \in \{0, 1\}$ is as explained above, and

$$l_{i,\infty}(C, Y_0, \dots, Y_{n-1}) := Y_{i-1} \quad \text{for } i \in \{1, \dots, n\}.$$

For all other places v in S , we define

$$l_{0,v} := C, \quad l_{i,v} := Y_{i-1} \quad \text{for } i = 1, \dots, n.$$

We will show that there is some $\delta > 0$, such that the inequality

$$\prod_{v \in S} \prod_{i=0}^n \frac{|l_{i,v}(\mathbf{y})|_v}{|\mathbf{y}|_v} < \left(\prod_{v \in S} |\det(l_{0,v}, \dots, l_{n,v})|_v \right) \cdot \mathcal{H}(\mathbf{y})^{-(n+1)-\delta} \quad (16)$$

is satisfied for all vectors

$$\mathbf{y} = \left(c, \alpha_1^{(-x+y+z-\epsilon)/2}, \alpha_1^{(-x+y+z-\epsilon)/2} M_1, \dots, \alpha_1^{(-x+y+z-\epsilon)/2} M_{n-1} \right).$$

The use of the correct $\epsilon \in \{0, 1\}$ guarantees that these vectors are indeed in \mathbb{L}^n .

First, notice that the determinant in (16) equals 1 for all places v . Thus (16) reduces to

$$\prod_{v \in S} \prod_{i=0}^n \frac{|l_{i,v}(\mathbf{y})|_v}{|\mathbf{y}|_v} < \mathcal{H}(\mathbf{y})^{-(n+1)-\delta},$$

and the double product on the left-hand side can be split up into

$$|c - \sqrt{f_1 \alpha_1^\epsilon} y_0 - \sqrt{f_1 \alpha_1^\epsilon} \sum_{j=1}^{n-1} d_j y_j|_\infty \cdot \prod_{v \in M_{\mathbb{L}, \infty}, v \neq \infty} |c|_v \cdot \prod_{v \in S \setminus M_{\mathbb{L}, \infty}} |c|_v \cdot \prod_{j=1}^{n-1} \prod_{v \in S} |y_j|_v.$$

Now notice that the last double product equals 1 due to the Product Formula and that

$$\prod_{v \in S \setminus M_{\mathbb{L}, \infty}} |c|_v \leq 1,$$

since $c \in \mathbb{Z}$. An upper bound on the number of infinite places in \mathbb{L} is $k!$ and hence

$$\begin{aligned} \prod_{v \in M_{\mathbb{L}, \infty}, v \neq \infty} |c|_v &< \left(\frac{(T_y - 1)(T_z - 1)}{T_x - 1} \right)^{k!} \\ &\leq (f_1 \alpha_1^y + \dots + f_k \alpha_k^y - 1)^{k!} (f_1 \alpha_1^z + \dots + f_k \alpha_k^z - 1)^{k!} \\ &\leq (1 \cdot 2^{\|x\|} + 1/2)^{2 \cdot k!} \end{aligned}$$

using (6) and (5). And finally the first expression is just

$$\left| \sqrt{f_1 \alpha_1^\epsilon} \alpha^{(-x+y+z-\epsilon)/2} \sum_{j \geq n} d_j M_j \right|,$$

which, by (13), is smaller than some expression of the form $C_2 \alpha_1^{T\|x\|/C_1}$. Therefore, we have

$$\prod_{v \in S} \prod_{i=0}^n \frac{|l_{i,v}(\mathbf{y})|_v}{|\mathbf{y}|_v} < C_2 \alpha_1^{T\|x\|/C_1} \cdot (2^{\|x\|} + 1/2)^{2 \cdot k!}.$$

Now we choose T (and the corresponding n) in such a way that

$$C_2 \alpha_1^{-T\|x\|/C_1} < \alpha_1^{-\frac{T\|x\|}{2C_1}}$$

and

$$(2^{\|x\|} + 1/2)^{2 \cdot k!} < \alpha_1^{\frac{T\|x\|}{4C_1}}$$

holds. Then we can write

$$\prod_{v \in S} \prod_{i=0}^n \frac{|l_{i,v}(\mathbf{y})|_v}{|\mathbf{y}|_v} < \alpha_1^{-\frac{T\|x\|}{2C_1}}. \quad (17)$$

For the height of our vector \mathbf{y} , we estimate

$$\begin{aligned} \mathcal{H}(\mathbf{y}) &\leq C_3 \cdot \mathcal{H}(c) \cdot \mathcal{H}\left(\alpha_1^{\frac{-x+y+z-\epsilon}{2}}\right)^n \cdot \prod_{i=1}^{n-1} \mathcal{H}(M_j) \\ &\leq C_3 (2^{\|x\|} + 1/2)^{k!} \prod_{i=1}^{n-1} \alpha_1^{C_4 \|x\|} \\ &\leq \alpha_1^{C_5 \|x\|}, \end{aligned}$$

with suitable constants C_3, C_4, C_5 . For the second estimate, we used that

$$\mathcal{H}(M_j) \leq \mathcal{H}(\alpha_1)^{C_{\alpha_1}(\mathbf{x})} \mathcal{H}(\alpha_2)^{C_{\alpha_2}(\mathbf{x})} \dots \mathcal{H}(\alpha_k)^{C_{\alpha_k}(\mathbf{x})}$$

and bounded it by the maximum of those expressions. Furthermore we have

$$\mathcal{H}\left(\alpha_1^{\frac{-x+y+z-\epsilon}{2}}\right)^n \leq \alpha_1^{n\|x\|},$$

which just changes our constant C_4 .

Now finally, the estimate

$$\alpha_1^{-\frac{T\|x\|}{2C_1}} \leq \alpha_1^{-\delta C_5 \|x\|}$$

is satisfied when we pick δ small enough.

So all the conditions for the Subspace theorem are met. Since we assumed that there are infinitely many solutions (x, y, z) of (16), we now can conclude that all of them lie in finitely many proper linear subspaces. Therefore, there must be at least one proper linear subspace, which contains infinitely many solutions and we see that there exists a finite set J and (new) coefficients e_j for $j \in J$ in \mathbb{L} such that we have

$$c = \alpha_1^{(-x+y+z-\epsilon)/2} \left(e_0 + \sum_{j \in J_c} e_j M_j \right) \quad (18)$$

with (new) non-zero coefficients e_j and monomials M_j as before.

Likewise, we can find finite expressions of this form for a and b .

4 Proof of the Theorem

We use the following parametrization lemma:

Lemma 3 *Suppose, we have infinitely many solutions for (1). Then there exists a line in \mathbb{R}^3 given by*

$$x(t) = r_1 t + s_1, \quad y(t) = r_2 t + s_2, \quad z(t) = r_3 t + s_3$$

with rationals $r_1, r_2, r_3, s_1, s_2, s_3$, such that infinitely many of the solutions (x, y, z) are of the form $(x(n), y(n), z(n))$ for some integer n .

Proof Assume that (1) has infinitely many solutions. We already deduced in Sect. 3 that c can be written in the form

$$c = \alpha_1^{(-x+y+z-\epsilon)/2} \left(e_{c,0} + \sum_{j \in J_c} e_{c,j} M_{c,j} \right)$$

with J_c being a finite set, $e_{c,j}$ being coefficients in \mathbb{L} for $j \in J_c \cup \{0\}$ and $M_{c,j} = \prod_{i=1}^k \alpha_i^{L_{c,i,j}(\mathbf{x})}$ with $\mathbf{x} = (x, y, z)$. In the same manner, we can write

$$b = \alpha_1^{(x-y+z-\epsilon)/2} \left(e_{b,0} + \sum_{j \in J_b} e_{b,j} M_{b,j} \right).$$

Since $1 + bc = F_z = f_1 \alpha_1^z + \dots + f_k \alpha_k^z$, we get

$$f_1 \alpha_1^z + \dots + f_k \alpha_k^z - \alpha_1^{z-\epsilon} \left(e_{b,0} + \sum_{j \in J_b} e_{b,j} M_{b,j} \right) \left(e_{c,0} + \sum_{j \in J_c} e_{c,j} M_{c,j} \right) = 1. \quad (19)$$

Substituting

$$\alpha_k = \frac{(-1)^{k-1}}{\alpha_1 \cdots \alpha_{k-1}}$$

into (19), we obtain an equation of the form

$$\sum_{j \in J} e_j \alpha_1^{L_{1,j}(\mathbf{x})} \cdots \alpha_{k-1}^{L_{k-1,j}(\mathbf{x})} = 0, \quad (20)$$

where again J is some finite set, e_j are non-zero coefficients in \mathbb{L} and $L_{i,j}$ are linear forms in \mathbf{x} with integer coefficients.

This is an S -unit equation, where S is the multiplicative group generated by $\{\alpha_1, \dots, \alpha_k, -1\}$. We may assume that infinitely many of the solutions \mathbf{x} are non-degenerate solutions of (20) by replacing the equation by an equation given by a suitable vanishing subsum if necessary.

We may assume that $(L_{1,i}, \dots, L_{k-1,i}) \neq (L_{1,j}, \dots, L_{k-1,j})$ for any $i \neq j$, because otherwise we could just merge these two terms.

Therefore for $i \neq j$, the theorem on non-degenerate solutions to S -unit equations (see [6]) yields that the set of

$$\alpha_1^{L_{1,i}(\mathbf{x}) - L_{1,j}(\mathbf{x})} \cdots \alpha_{k-1}^{L_{k-1,i}(\mathbf{x}) - L_{k-1,j}(\mathbf{x})}$$

is contained in a finite set of numbers. By Lemma 1, $\alpha_1, \dots, \alpha_{k-1}$ are multiplicatively independent and thus the exponents $(L_{1,i} - L_{1,j})(\mathbf{x}), \dots, (L_{k-1,i} - L_{k-1,j})(\mathbf{x})$ take the same value for infinitely many \mathbf{x} . Since we assumed that these linear forms are not all identically zero, this implies that there is some non-trivial linear form L defined over \mathbb{Q} and some $c \in \mathbb{Q}$ with $L(\mathbf{x}) = c$ for infinitely many \mathbf{x} . So there exist rationals r_i, s_i, t_i for $i = 1, 2, 3$ such that we can parametrize

$$x = r_1 p + s_1 q + t_1, \quad y = r_2 p + s_2 q + t_2, \quad z = r_3 p + s_3 q + t_3$$

with infinitely many pairs $(p, q) \in \mathbb{Z}^2$.

We can assume that r_i, s_i, t_i are all integers. If not, we define Δ as the least common multiple of the denominators of r_i, s_i ($i = 1, 2, 3$) and let p_0, q_0 be such that for infinitely many pairs (p, q) we have $p \equiv p_0 \pmod{\Delta}$ and $q \equiv q_0 \pmod{\Delta}$. Then $p = p_0 + \Delta\lambda, q = q_0 + \Delta\mu$ and

$$\begin{aligned} x &= (r_1 \Delta)\lambda + (s_1 \Delta)\mu + (r_1 p_0 + s_1 q_0 + t_1) \\ y &= (r_2 \Delta)\lambda + (s_2 \Delta)\mu + (r_2 p_0 + s_2 q_0 + t_2) \\ z &= (r_3 \Delta)\lambda + (s_3 \Delta)\mu + (r_3 p_0 + s_3 q_0 + t_3). \end{aligned}$$

Since $r_i \Delta, s_i \Delta$ and x, y, z are all integers, $r_i p_0 + s_i q_0 + t_i$ are integers as well. Replacing r_i by $r_i \Delta, s_i$ by $s_i \Delta$ and t_i by $r_i p_0 + s_i q_0 + t_i$, we can indeed assume that all coefficients r_i, s_i, t_i in our parametrization are integers.

Using a similar argument as in the beginning of the proof, we get that our equation is of the form

$$\sum_{j \in J} e'_j \alpha_1^{L'_{1,j}(\mathbf{r})} \cdots \alpha_{k-1}^{L'_{k-1,j}(\mathbf{r})} = 0,$$

where $\mathbf{r} := (\lambda, \mu)$, J is a finite set of indices, e'_j are new non-zero coefficients in \mathbb{L} and $L'_{i,j}(\mathbf{r})$ are linear forms in \mathbf{r} with integer coefficients. Again we may assume that we have $(L'_{1,i}(\mathbf{r}), \dots, L'_{k-1,i}(\mathbf{r})) \neq (L'_{1,j}(\mathbf{r}), \dots, L'_{k-1,j}(\mathbf{r}))$ for any $i \neq j$.

Applying the theorem of non-degenerate solutions to S -unit equations once more, we obtain a finite set of numbers Λ , such that for some $i \neq j$, we have

$$\alpha_1^{(L'_{1,i}-L'_{1,j})(\mathbf{r})} \cdots \alpha_{k-1}^{(L'_{k-1,i}-L'_{k-1,j})(\mathbf{r})} \in \Lambda.$$

So every \mathbf{r} lies on a finite collection of lines and since we had infinitely many \mathbf{r} , there must be some line, which contains infinitely many solution, which proves our lemma. \square

We apply this lemma and define Δ as the least common multiple of the denominators of r_1, r_2, r_3 . Infinitely many of our n will be in the same residue class modulo Δ , which we shall call r . Writing $n = m\Delta + r$, we get

$$(x, y, z) = ((r_1\Delta)m + (rr_1 + s_1), (r_2\Delta)m + (rr_2 + s_2), (r_3\Delta)m + (rr_3 + s_3)).$$

Replacing n by m , r_i by $r_i\Delta$ and s_i by $rr_i + s$, we can even assume that r_i, s_i are integers. So we have

$$\frac{-x + y + z - \epsilon}{2} = \frac{(-r_1 + r_2 + r_3)m}{2} + \frac{-s_1 + s_2 + s_3 - \epsilon}{2}.$$

This holds for infinitely many m , so we can choose a still infinite subset such that all of them are in the same residue class δ modulo 2 and we can write $m = 2\ell + \delta$ with fixed $\delta \in \{0, 1\}$. Thus we have

$$\frac{-x + y + z - \epsilon}{2} = (-r_1 + r_2 + r_3)\ell + \eta,$$

where $\eta \in \mathbb{Z}$ or $\eta \in \mathbb{Z} + 1/2$.

Using this representation, we can write (18) as

$$c(\ell) = \alpha_1^{(-r_1+r_2+r_3)\ell+S} \left(e_0 + \sum_{j \in J_c} e_j M_j \right). \quad (21)$$

for infinitely many ℓ , where

$$M_j = \prod_{i=1}^k \alpha_i^{L_{i,j}(\mathbf{x})},$$

as before and $\mathbf{x} = \mathbf{x}(\ell) = (x(2\ell + \delta), y(2\ell + \delta), z(2\ell + \delta))$. From this, we will now derive a contradiction.

First we observe that there are only finitely many solutions of (21) with $c(\ell) = 0$. This can be shown by using the fact that a simple non-degenerate linear recurrence has only finite zero-multiplicity (see [6] for an explicit bound). We will apply this statement here for the linear recurrence in ℓ ; it only remains to check that no quotient of two distinct roots of the form $\alpha_1^{L_{1,i}(\mathbf{x}(\ell))} \cdots \alpha_k^{L_{k,i}(\mathbf{x}(\ell))}$ is a root of unity or, in other words, that

$$(\alpha_1^{m_1} \alpha_2^{m_2} \cdots \alpha_k^{m_k})^n = 1 \quad (22)$$

has no solutions in $n \in \mathbb{Z}/\{0\}$, $m_1 < 0$ and $m_i > 0$ for $i = 2, \dots, k$. Assume relation (22) holds. Replacing α_1 by $(-1)^{k-1}(\alpha_2 \cdots \alpha_k)^{-1}$ gives

$$\alpha_2^{2(m_2 - m_1)} \cdots \alpha_k^{2(m_k - m_1)} = 1.$$

By squaring this equation and applying Lemma 1 we get $2(m_2 - m_1) = \cdots = 2(m_k - m_1) = 0$ and thus $m_1 = m_2 = \cdots = m_k$, which is impossible because of the signs of m_1 and m_2, \dots, m_k .

So we have confirmed that $c(\ell) \neq 0$ for still infinitely many solutions. We use (12) and write

$$(F_x - 1)c^2 = (F_y - 1)(F_z - 1). \quad (23)$$

Then we insert the finite expansion (21) in ℓ for c into (23). Furthermore, we use the Binet formula (3) and write F_x, F_y, F_z as power sums in x, y and z respectively. Using the parametrization $(x, y, z) = (r_1 m + s_1, r_2 m + s_2, r_3 m + s_3)$ with $m = 2\ell$ or $m = 2\ell + 1$ as above, we have expansions in ℓ on both sides of (3). Since there must be infinitely many solutions in ℓ , the largest terms on both sides have to grow with the same rate. In order to find the largest terms, we have to distinguish some cases: If we assume that $e_0 \neq 0$ for infinitely many of our solutions, then $e_0 \alpha_1^{(-x+y+z-\epsilon)/2}$ is the largest term in the expansion of c and we have

$$f_1 \alpha_1^x e_0^2 \alpha_1^{-x+y+z-\epsilon} = f_1 \alpha_1^y f_1 \alpha_1^z.$$

It follows that $e_0^2 = f_1 \alpha_1^\epsilon$. The case $e_0 = 0$ for infinitely many of our solutions is not possible, because then, the right-hand side of (23) would grow faster than the left-hand side so that (23) could be true for only finitely many of our ℓ . In the other cases, we have $e_0 = \sqrt{f_1} \alpha_1^\epsilon$, where $\epsilon \in \{0, 1\}$. This now contradicts the following lemma, which turns out to be slightly more involved than in the special case on Tribonacci numbers (cf. [8]).

Lemma 4 $\sqrt{f_1} \notin \mathbb{L}$ and $\sqrt{f_1\alpha_1} \notin \mathbb{L}$.

Proof Suppose that $\sqrt{f_1\alpha_1^\epsilon} \in \mathbb{L}$ for some $\epsilon \in \{0, 1\}$. Then there is $\beta \in \mathbb{L}$ such that $f_1\alpha_1^\epsilon = \beta^2$. Using (4), we get that

$$\frac{(\alpha_1 - 1)\alpha_1^{-\epsilon}}{2 + (k + 1)(\alpha_1 - 2)} = \beta^2.$$

Computing norms over \mathbb{Q} , we get that

$$\left| \frac{N_{\mathbb{L}/\mathbb{Q}}(\alpha_1)^{-\epsilon} N_{\mathbb{L}/\mathbb{Q}}(\alpha_1 - 1)}{N_{\mathbb{L}/\mathbb{Q}}(2 + (k + 1)(\alpha_1 - 2))} \right| = N_{\mathbb{L}/\mathbb{Q}}(\beta)^2 = \square, \quad (24)$$

where \square denotes a rational square. Note that

$$|N_{\mathbb{L}/\mathbb{Q}}(\alpha_1)| = \left| \prod_{i=1}^k \alpha_i \right| = |(-1)^k \cdot (-1)| = 1,$$

and

$$|N_{\mathbb{L}/\mathbb{Q}}(\alpha_1 - 1)| = \left| \prod_{i=1}^k (\alpha_i - 1) \right| = |\Psi_k(1)| = k - 1,$$

and finally that

$$\begin{aligned} |N_{\mathbb{L}/\mathbb{Q}}(2 + (k + 1)(\alpha_1 - 2))| &= |N_{\mathbb{L}/\mathbb{Q}}((k + 1)\alpha_1 - 2k)| \\ &= \left| \prod_{i=1}^k ((k + 1)\alpha_i - 2k) \right| \\ &= (k + 1)^k \left| \prod_{i=1}^k (2k/(k + 1) - \alpha_i) \right| \\ &= (k + 1)^k |\Psi_k(2k/(k + 1))| \\ &= (k + 1)^k \left| \frac{X^{k+1} - 2X^k + 1}{X - 1} \right|_{X=2k/(k+1)} \\ &= \frac{2^{k+1}k^k - (k + 1)^{k+1}}{k - 1}. \end{aligned}$$

Hence, we get that equation (24) leads to

$$\frac{2^{k+1}k^k - (k + 1)^{k+1}}{(k - 1)^2} = \square.$$

This leads to

$$2^{k+1}k^k - (k + 1)^{k+1} = w^2 \quad (25)$$

for some integer w . But this equation has no integer solutions, which is proved in the theorem below. This concludes the proof. \square

In order to finish the proof, we have the following result, which might be of independent interest since particular cases were considered before in [2] and [16].

Theorem 2 *The Diophantine equation (25) has no positive integer solutions (k, w) with $k \geq 2$.*

Proof The cases $k \equiv 1, 2 \pmod{4}$ have already been treated both in [2] and in [16]. We treat the remaining cases. If $k \equiv 0 \pmod{4}$, then the left-hand side of (25) is congruent to $-1 \pmod{4}$, and therefore it cannot be a square. Finally, assume that $k \equiv 3 \pmod{4}$. Then $k + 1$ is even, $2^{(k+1)/2} \mid w$, and putting $w_1 = w/2^{(k+1)/2}$, we get

$$k^k - ((k+1)/2)^{k+1} = w_1^2.$$

We then get

$$k^k = w_1^2 + ((k+1)/2)^{k+1}. \quad (26)$$

Note that the two numbers in the right-hand side of (26) are coprime, for if p divides w_1 and $(k+1)/2$, then p divides the left-hand side of (26). Thus p divides both k and $(k+1)/2$, so also $k - 2((k+1)/2) = -1$, a contradiction. Thus, the right-hand side is a sum of two coprime squares and therefore all odd prime factors of it must be 1 modulo 4 contradicting the fact that in the left-hand side we have $k \equiv 3 \pmod{4}$. This finishes the proof of this theorem. \square

Acknowledgements Open access funding provided by University of Salzburg. C.F. and C.H. were supported by FWF (Austrian Science Fund) Grant No. P24574 and by the Sparkling Science project EMMA Grant No. SPA 05/172.

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

1. Bravo, J.J., Luca, F.: On a conjecture about repdigits in k -generalized Fibonacci sequences. *Publ. Math. Debrecen* **82**, 623–639 (2013)
2. Cipu, M., Luca, F.: On the Galois group of the generalized Fibonacci polynomial. *Ann. Șt. Univ. Ovidius Constanța* **9**, 27–38 (2001)
3. Dresden, G.P., Du, Z.: A simplified Binet formula for k -generalized Fibonacci numbers. *J. Integer Sequences* **17**, Article 14.4.7 (2014)
4. Dujella, A.: There are only finitely many Diophantine quintuples. *J. Reine Angew. Math.* **566**, 183–214 (2004)
5. Evertse, J.-H.: An improvement of the quantitative Subspace Theorem. *Compos. Math.* **101**, 225–311 (1996)
6. Evertse, J.-H., Schmidt, W., Schlickewei, H.-P.: Linear equations in variables which lie in a multiplicative group. *Ann. Math.* **2**(155), 807–836 (2002)

7. Fuchs, C., Luca, F., Szalay, L.: Diophantine triples with values in binary recurrences. *Ann. Sc. Norm. Super. Pisa Cl. Sc.* **5**(7), 579–608 (2008)
8. Fuchs, C., Hutle, C., Irmak, N., Luca, F., Szalay, L.: Only finitely many Tribonacci Diophantine triples exist. To appear in *Math. Slovaca*; [arXiv:1508.07760](https://arxiv.org/abs/1508.07760)
9. Fuchs, C., Tichy, R.F.: Perfect powers in linear recurrence sequences. *Acta Arith.* **107**(1), 9–25 (2003)
10. Fuchs, C.: Polynomial-exponential equations and linear recurrences. *Glas. Mat. Ser. III* **38**(58), 233–252 (2003)
11. Gomez Ruiz, C.A., Luca, F.: Tribonacci Diophantine quadruples. *Glas. Mat.* **50**(1), 17–24 (2015)
12. Irmak, N., Szalay, L.: Diophantine triples and reduced quadruples with the Lucas sequence of recurrence $u_n = Au_{n-1} - u_{n-2}$. *Glas. Mat.* **49**, 303–312 (2014)
13. Luca, F., Szalay, L.: Fibonacci Diophantine triples. *Glas. Mat.* **43**(63), 253–264 (2008)
14. Luca, F., Szalay, L.: Lucas Diophantine triples. *Integers* **9**, 441–457 (2009)
15. Mignotte, M.: Sur les conjugués des nombres de Pisot, C. R. Acad. Sci. Paris Sér. I Math. **298**(2), 21 (1984)
16. Martin, P.A.: The Galois group of $X^n - X^{n-1} - \dots - 1$. *J. Pure App. Algebra* **190**, 213–223 (2004)
17. Neukirch, J.: *Algebraic Number Theory*. Springer, New York (1999)
18. Szalay, L., Ziegler, V.: On an S -unit variant of Diophantine m -tuples. *Publ. Math. Debrecen* **83**, 97–121 (2013)